UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/005,105 | 12/03/2001 | Paul C. Kocher | 44424162-8721 | 1675 |

26263 7590 10/05/2007

SONNENSCHEIN NATH & ROSENTHAL LLP
P.O. BOX 061080
WACKER DRIVE STATION, SEARS TOWER
CHICAGO, IL 60606-1080

| EXAMINER | |
|---|---|
| NOBAHAR, ABDULHAKIM | |
| **ART UNIT** | **PAPER NUMBER** |
| 2132 | |
| **MAIL DATE** | **DELIVERY MODE** |
| 10/05/2007 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/005,105 | KOCHER ET AL. | |
| | Examiner | Art Unit | |
| | Abdulhakim Nobahar | 2132 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *06 August 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *09/17/2007, 08/06/2007*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

### *Requirement For Information - 37 CFR 1.105*

Applicant and the assignee of this application are required under 37 CFR 1.105 to provide the following information that the examiner has determined is reasonably necessary to the examination of this application:

On May 04, 2007 applicants filed an IDS with three items one of which is a DVD (United States Air Force Audio Visual Presentation). Further, there were twenty other documents filed entitled "Exhibits", without explanation and unlisted on any 1499 form. Applicants are required to provide information to explain the nature of these "Exhibits", identity of the litigation (if any) relating to these items and their relation to the instant application.

### *Claim Rejections - 35 USC § 102*

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

**Claims 1-19 are rejected under 35 U.S.C. 102(e) as being anticipated by Gressel et al (6,748,410 B1; hereinafter Gressel)**

Regarding claim 1-3, 12 and 13, Gressel discloses:

A method for evaluating the security of a cryptographic device to recover useful information about a key, said device containing at least said key and a circuit configured

to perform cryptographic operations using said key (see, for example, col. 3, lines 25-39), said method comprising:

a) connecting said device (col. 1, lines 47-54 and col. 3, lines 14-19) to an analog-to-digital converter (col. 50, lines 58-64; col. 53, lines 45-48) configured to measure an attribute (col. 13, lines 24-36, where the current dissipation corresponds to the recited attribute or to the recited electromagnetic radiation; col. 21, lines 15-35; col. 22, lines 5-20, where the current consumption correspond to the recited power consumotion) related to operation of said device (col. 1, lines 61-65);

(b) sending a plurality of command sequences to said device, where each said command sequence causes said device to perform a cryptographic operation to process data using said key (col. 10, lines 62-66; col. 51, lines 38-44);

(c) during processing of each said cryptographic operation, recording a plurality of measurements of said attribute by using said analog-to-digital converter (col. 21, lines 29-35; col. 23, lines 21-31); and

(d) determining whether information about said key is leaking from said device by statistically combining said recorded measurements (col. 13, lines 28-36; col. 23, lines 24-32; col. 51, lines 38-44).

Regarding claim 18, this claim is rejected as applied to the like elements of claims 1-3 as indicated above and further the following:

(e) computing the alignment of said measurements in said plurality of sets such that measurements corresponding to a single point of interest can be compared (col. 25,

lines 20-26, where detecting position corresponds to the recited computing the alignment; col. 53, lines 40-48, where to accurately estimate the placement corresponds to the recited computing the alignment);

(f) generating a guess of a value of a portion of said key (col. 53, lines 40-48; col. 59, lines 39-43, where estimate on the number corresponds to the recited guess of a value);

(g) using said guess, computing an average of a subset of said aligned measurements (col. 20, lines 39-47; col. 24, lines 55-59; col. 59, lines 44-51); and

(h) verifying correctness of said guess by detecting existence of a bias in said average (col. 8, lines 45-50; col. 23, lines 40-44; col. 53, lines 20-27).

Regarding claims 4, 5 and 15, Gressel discloses:

The method of claim 3 where said cryptographic operation includes transforming with a block cipher (col. 13, lines 20-25; col. 51, lines 1-3, where the crypto-operations could include a block cipher or DES).

Regarding claim 6, Gressel discloses:

The method of claim 5 where said data includes an input to said DES block cipher operation (col. 2, lines 48-53).

Regarding claim 7, Gressel discloses:

The method of claim 5 where said data includes an output from said DES block cipher operation (col. 6, lines 10-12; col. 6, lines 43-67; col. 16, lines 57-65).

Regarding claims 8 and 16, Gressel discloses:

The method of claim 2 where said step (d) further includes determining information about said key (col. 13, line 30).

Regarding claim 9, Gressel discloses:

The method of claim 8 where said information about said key is usable to reduce an amount of effort required for a brute force attack against said key (col. 20, line 39-47).

Regarding claim 10, Gressel discloses:

The method of claim 9 where said information about said key includes values of a plurality of key bits (col. 22, lines 44-55; col. 23, lines 5-20).

Regarding claims 11 and 17, Gressel discloses:

The method of claim 1 further comprising temporally aligning data points corresponding to a point of interest within said plurality of measurements (col. 8, lines 37-43; col. 9, lines 27-36; col. 50, lines 50-57).

Regarding claims 14 and 19, Gressel discloses:

The system of claim 12 where said attribute includes variations in an amount of power consumed on an external power input to said device (col. 21, lines 29-42; col. 22, lines 2-20; col. 54, lines 25-34).

***Conclusion***

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. Patent No. 7,073,072 B1 to Salle.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Abdulhakim Nobahar whose telephone number is 571-272-3808. The examiner can normally be reached on M-T 8-6.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Abdulhakim Nobahar
Examiner
Art Unit 2132 A.N.

September 7, 2007

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100